PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224456
(43)Date of publication of application : 17.08.1999

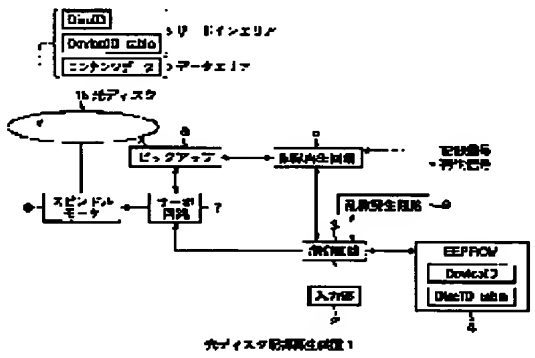
(51)Int.Cl. G11B 19/04
G06F 3/06
G06F 12/14
G11B 19/12
G11B 20/10
G11B 20/12

(21)Application number : 10-025311
(22)Date of filing : 06.02.1998

(71)Applicant : SONY CORP
(72)Inventor : ASANO TOMOYUKI

(54) INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, PROVIDING MEDIUM AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the illegal copying of information recorded in a recording medium.
SOLUTION: A control circuit 3 reads the DiscID of an optical disk 15. A random number generating circuit 9 generates a specified random number changed for each access. The control circuit 3 writes the read DiscID of the optical disk 15 and the random number in the DiscID table of an EEPROM 4. The control circuit 3 also writes the DeviceID of an optical disk recording/ reproducing device 1 and the same random number as that described above in the DeviceID table of the optical disk 15. The control circuit 3 reads the DeviceID table and, if the read random number is not coincided with that of the corresponding DiscID table, rejects access to the user data area of the optical disk 15.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－224456

(43)公開日　平成11年(1999)８月17日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ１１Ｂ	19/04	５０１	Ｇ１１Ｂ	19/04	５０１Ｈ
Ｇ０６Ｆ	3/06	３０４	Ｇ０６Ｆ	3/06	３０４Ｍ
	12/14	３２０		12/14	３２０Ｆ
Ｇ１１Ｂ	19/12	５０１	Ｇ１１Ｂ	19/12	５０１Ｋ
	20/10			20/10	Ｈ

審査請求　未請求　請求項の数４　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平10－25311

(22)出願日　平成10年(1998)２月６日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

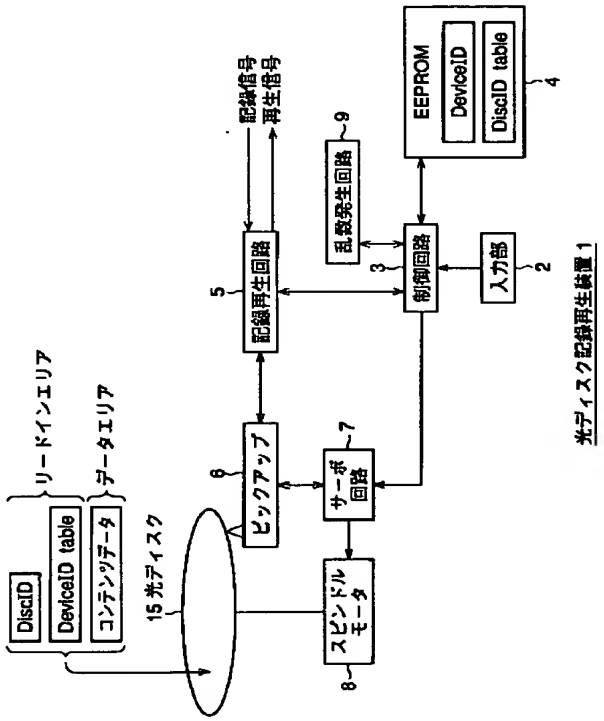
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　情報処理装置、情報処理方法、提供媒体、および記録媒体

(57)【要約】

【課題】　記録媒体に記録された情報が不正にコピーされるのを防止する。

【解決手段】　制御回路３は、光ディスク１５のDiscIDを読み出す。乱数発生回路９は、アクセス毎に変化する所定の乱数を発生させる。制御回路３は、読み出した光ディスク１５のDiscIDおよび乱数を、EEPROM４のDiscID tableに書き込む。制御回路３はまた、光ディスク記録再生装置１のDeviceID、および上述したものと同一の乱数を、光ディスク１５のDeviceID tableに書き込む。制御回路３は、DeviceID tableを読み出し、読み出された乱数が、対応するDiscID tableのものと一致しない場合には、光ディスク１５のユーザデータエリアへのアクセスを拒絶する。



【特許請求の範囲】
【請求項１】　着脱可能な記録媒体に情報を記録または再生する情報処理装置において、
前記記録媒体のIDを読み出す第１の読出手段と、
所定の時変情報を発生する発生手段と、
前記第１の読出手段により読み出された前記記録媒体のID、および、前記発生手段が発生した前記時変情報を、互いに対応させて第１のテーブルに記憶させる記憶手段と、
前記記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、前記発生手段が発生した前記時変情報を、互いに対応させて、前記記録媒体の第２のテーブルに記録させる記録手段と、
前記記録媒体の第２のテーブルを読み出す第２の読出手段と、
前記第１のテーブルの内容と、第２の読出手段が読み出した前記第２のテーブルの内容を比較し、その比較結果に対応して前記記録媒体に対するアクセスを制御する制御手段とを備えることを特徴とする情報処理装置。
【請求項２】　着脱可能な記録媒体に情報を記録または再生する情報処理方法において、
前記記録媒体のIDを読み出す第１の読出ステップと、
所定の時変情報を発生する発生ステップと、
前記第１の読出ステップで読み出された前記記録媒体のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて第１のテーブルに記憶させる記憶ステップと、
前記記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて、前記記録媒体の第２のテーブルに記録させる記録ステップと、
前記記録媒体の第２のテーブルを読み出す第２の読出ステップと、
前記第１のテーブルの内容と、前記第２の読出ステップで読み出した前記第２のテーブルの内容を比較し、その比較結果に対応して前記記録媒体に対するアクセスを制御する制御ステップとを備えることを特徴とする情報処理方法。
【請求項３】　着脱可能な記録媒体に情報を記録または再生する情報処理装置に使用するコンピュータプログラムであって、
前記記録媒体のIDを読み出す第１の読出ステップと、
所定の時変情報を発生する発生ステップと、
前記第１の読出ステップで読み出された前記記録媒体のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて第１のテーブルに記憶させる記憶ステップと、
前記記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、前記発生ステップで発生した前記時変情報を、互いに対応させて、前記記録媒体の第２のテーブルに記録させる記録ステップと、
前記記録媒体の第２のテーブルを読み出す第２の読出ステップと、
前記第１のテーブルの内容と、前記第２の読出ステップで読み出した前記第２のテーブルの内容を比較し、その比較結果に対応して前記記録媒体に対するアクセスを制御する制御ステップとを備えるコンピュータプログラムを提供することを特徴とする提供媒体。
【請求項４】　情報処理装置に装着され、情報が記録または再生される記録媒体において、
前記記録媒体に固有のIDと、
装着された前記情報処理装置のIDと、
前記情報処理装置が発生した時変情報とが記録されていることを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、提供媒体、および記録媒体に関し、特に、より安全にデータを授受することを可能にする情報処理装置、情報処理方法、提供媒体、および記録媒体に関する。
【０００２】
【従来の技術】近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまうおそれがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。
【０００３】例えば、ミニディスク（MD）（商標）システムにおいては、SCMS(Serial CopyManagement System)と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free,copy once allowed,またはcopy prohibitedのうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。
【０００４】このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００５】また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号を復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００６】

【発明が解決しようとする課題】しかしながら、上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録機器が、不正に製造されてしまう。

【０００７】また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。なぜなら、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【０００８】本発明はこのような状況に鑑みてなされたものであり、記録媒体のIDおよび所定の時変情報を記憶するとともに、記録媒体にアクセスした装置のIDおよび時変情報を記録媒体に記録させ、両者の情報の履歴に基づいてアクセスを制御することで、より安全にデータを授受することを可能にするものである。

【０００９】

【課題を解決するための手段】請求項１に記載の情報処理装置は、記録媒体のIDを読み出す第１の読出手段と、所定の時変情報を発生する発生手段と、第１の読出手段により読み出された記録媒体のID、および、発生手段が発生した時変情報を、互いに対応させて第１のテーブルに記憶させる記憶手段と、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生手段が発生した時変情報を、互いに対応させて、記録媒体の第２のテーブルに記録させる記録手段と、記録媒体の第２のテーブルを読み出す第２の読出手段と、第１のテーブルの内容と、第２の読出手段が読み出した第２のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御手段とを備えることを特徴とする。

【００１０】請求項２に記載の情報処理方法は、記録媒体のIDを読み出す第１の読出ステップと、所定の時変情報を発生する発生ステップと、第１の読出ステップで読み出された記録媒体のID、および、発生ステップで発生した時変情報を、互いに対応させて第１のテーブルに記憶させる記憶ステップと、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生ステップで発生した時変情報を、互いに対応させて、記録媒体の第２のテーブルに記録させる記録ステップと、記録媒体の第２のテーブルを読み出す第２の読出ステップと、第１のテーブルの内容と、第２の読出ステップで読み出した第２のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御ステップとを備えることを特徴とする。

【００１１】請求項３に記載の提供媒体は、記録媒体のIDを読み出す第１の読出ステップと、所定の時変情報を発生する発生ステップと、第１の読出ステップで読み出された記録媒体のID、および、発生ステップで発生した時変情報を、互いに対応させて第１のテーブルに記憶させる記憶ステップと、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生ステップで発生した時変情報を、互いに対応させて、記録媒体の第２のテーブルに記録させる記録ステップと、記録媒体の第２のテーブルを読み出す第２の読出ステップと、第１のテーブルの内容と、第２の読出ステップで読み出した第２のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御ステップとを備えるコンピュータプログラムを提供することを特徴とする。

【００１２】請求項４に記載の記録媒体は、記録媒体に固有のIDと、装着された情報処理装置のIDと、情報処理装置が発生した時変情報とが記録されていることを特徴とする。

【００１３】請求項１に記載の情報処理装置、請求項２に記載の情報処理方法、および請求項３に記載の提供媒体においては、記録媒体のIDが読み出され、所定の時変情報が発生され、読み出された記録媒体のID、および、発生された時変情報が、互いに対応して第１のテーブルに記憶される。また、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生した時変情報が、互いに対応して、記録媒体の第２のテーブルに記録され、記録媒体の第２のテーブルが読み出され、第１のテーブルの内容と、読み出された第２のテーブルの内容が比較され、その比較結果に対応して記録媒体に対するアクセスが制御される。

【００１４】請求項４に記載の記録媒体においては、記録媒体に固有のID、装着された情報処理装置のID、および情報処理装置が発生した時変情報とが記録される。

【００１５】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付

加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１６】請求項１に記載の情報処理装置は、記録媒体のIDを読み出す第１の読出手段（例えば、図４のステップＳ１）と、所定の時変情報を発生する発生手段（例えば、図４のステップＳ４）と、第１の読出手段により読み出された記録媒体のID、および、発生手段が発生した時変情報を、互いに対応させて第１のテーブルに記憶させる記憶手段（例えば、図４のステップＳ７，Ｓ８）と、記録媒体に対してアクセスした情報処理装置のIDとしての自分自身のID、および、発生手段が発生した時変情報を、互いに対応させて、記録媒体の第２のテーブルに記録させる記録手段（例えば、図４のステップＳ１１，Ｓ１２）と、記録媒体の第２のテーブルを読み出す第２の読出手段（例えば、図４のステップＳ１４）と、第１のテーブルの内容と、第２の読出手段が読み出した第２のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御する制御手段（例えば、図４のステップＳ１３，Ｓ１８，Ｓ１９）とを備えることを特徴とする。

【００１７】以下、本発明を、光ディスクにデータを記録または再生する光ディスク記録再生装置に適用した第１の実施の形態を、図面を参照しながら説明する。

【００１８】図１は、本発明を適用した光ディスク記録再生装置１の構成を示すブロック図である。入力部２は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。制御回路３は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。EEPROM４は、光ディスク記録再生装置１に固有なID（以下、DeviceIDと称する）、光ディスク記録再生装置１がアクセスした光ディスクの履歴としてのDiscID table、その他、装置の電源オフ後も記憶する必要のある情報を記憶する。

【００１９】記録再生回路５は、外部から記録信号の供給を受け取ると、これを変調し、ピックアップ６に供給して、装着された光ディスク１５に記録させる。記録再生回路５はまた、ピックアップ６により、光ディスク１５から再生されたデータを復調し、外部に再生信号として出力する。ピックアップ６は、レーザビームを光ディスク１５に照射することで、データの記録再生を行う。スピンドルモータ８は、サーボ回路７によって制御され、光ディスク１５を回転させる。

【００２０】サーボ回路７は、スピンドルモータ８を駆動することにより、光ディスク１５を所定の速度で（例えば線速度一定で）回転させる。サーボ回路７はまた、ピックアップ６のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。乱数発生回路９は、制御回路３の制御により、所定の乱数を発生する。光ディスク１５は、同図に示すように、通常のコンテンツデータの記録領域であるデータエリア以外に、リードインエリアを有する。リードインエリアには、光ディスクのID（以下、DiscIDと称する）と、光ディスク１５に対するアクセス履歴を記憶するDeviceID tableが記録される。

【００２１】図２は、DeviceID tableの具体例を示す図である。DeviceID tableは、内部に１００個のアドレスを有する。各アドレスには１乃至１００の所定のアドレス番号が対応し、１から１００まで昇順で、光ディスク１５にアクセスした装置のDeviceID、アクセス毎に発生された乱数（詳細は後述する）、および、（最終書き込みアドレスを示す）最終書き込みフラグが、アクセス毎に書き込まれる。なお、アドレス番号が１００に達したら、次は再び１に戻り、対応するデータも更新される。

【００２２】図３は、DiscID tableの具体例を示す図である。DiscID tableは、内部に１００個のアドレスを有する。各アドレスには１乃至１００の所定のアドレス番号が対応し、１から１００まで昇順で、光ディスク記録再生装置１がアクセスした光ディスクのDiscID、アクセス毎に発生した乱数、および、最終書き込みフラグが、アクセス毎に書き込まれる。なお、アドレス番号が１００に達したら、次は再び１に戻り、対応するデータも更新される。

【００２３】次に、光ディスク記録再生装置１の光ディスク１５に対するアクセスの動作について、図４のフローチャートを参照して説明する。最初にステップＳ１において、光ディスク記録再生装置１の制御回路３は、ピックアップ６を制御し、光ディスク１５のリードインエリアを再生させる。この再生信号は記録再生回路５により復調される。制御回路３はこの復調信号から、光ディスク１５のDiscIDとDeviceID tableを読み出し、記憶する。制御回路３は、ステップＳ２で、EEPROM４のDiscID tableに記憶されたデータを検索する。制御回路３は、ステップＳ３で、DiscID tableのデータの中に、ステップＳ１で読み出した光ディスク１５のDiscIDと一致するDiscIDがあるか否かを判定する。光ディスク１５のDiscIDと一致するDiscIDがないと判定された場合、ステップＳ４に進み、制御回路３は、乱数発生回路９を制御し、所定の乱数を発生させる。この乱数は、光ディスク記録再生装置１が光ディスク１５にアクセスする毎に、個別に発生する時変情報である。この乱数は、制御回路３に供給される。

【００２４】制御回路３は、ステップＳ５で、EEPROM４のDiscID tableを検索し、最終書き込みフラグを検出する。制御回路３は、ステップＳ６で、最終書き込みフラグが検出されたアドレスよりアドレス番号が１だけインクリメントされたアドレスを、今回のデータ書き込み位置（アドレス）として特定する。但し、アドレス番号は１００を超えることはなく、１００の次は再び１に戻る。制御回路３は、ステップＳ７で、ステップＳ１で読

み取ったDiscIDを、ステップＳ６で特定したアドレスに書き込む。さらに制御回路３はステップＳ８で、ステップＳ４で発生された乱数を、ステップＳ６で特定したアドレスに書き込むとともに、最終書き込みフラグを現在のアドレスに書き換える。これにより、DiscIDと乱数が対応して、DiscID tableに書き込まれたことになる。

【００２５】制御回路３は、ステップＳ９で、光ディスク１５のDeviceID table（ステップＳ１で読み出している）を検索し、最終書き込みフラグを検出する。制御回路３は、ステップＳ１０で、最終書き込みフラグが検出されたアドレスより、アドレス番号が１だけインクリメントされたアドレスを、今回のデータ書き込み位置（アドレス）として特定する。制御回路３は、ステップＳ１１で、EEPROM４から、光ディスク記録再生装置１のDeviceIDを読み出し、このDeviceIDを、記録再生回路５およびピックアップ６を介して、光ディスク１５のDeviceID tableの、ステップＳ１０で特定したアドレスに書き込ませる。

【００２６】制御回路３は、ステップＳ４で発生させた乱数を、記録再生回路５およびピックアップ６を介して、光ディスク１５のDeviceID tableの、ステップＳ１０で特定したアドレスに書き込ませるとともに、最終書き込みフラグを現在のアドレスに書き換えさせる。これにより、DeviceIDと乱数が対応してDeviceID tableに書き込まれたことになる。

【００２７】次に、ステップＳ１３に進み、制御回路３は、ピックアップ６を制御して、光ディスク１５の入力部２からの指令に対応するユーザデータエリアへアクセスさせ、記録または再生動作を実行させる。すなわち、この場合、制御回路３は、ユーザデータエリアへのアクセス（ユーザデータの記録または再生）を許容する。

【００２８】一方、ステップＳ３で、光ディスク１５から読み取ったDiscIDと同一のDiscIDが、EEPROM４のDiscID tableに既に記憶されていると判定された場合、ステップＳ１４に進み、制御回路３は、光ディスク１５のDeviceID tableを検索する。制御回路３は、ステップＳ１５で、光ディスク１５のDeviceID tableに、光ディスク記録再生装置１のDeviceIDが記録されているか否かを判定する。光ディスク記録再生装置１のDeviceIDが光ディスク１５のDeviceID tableに記録されていると判定された場合、ステップＳ１６に進み、制御回路３は、光ディスク１５のDeviceID tableから、ステップＳ１５でDeviceIDが検出されたのと同一のアドレスにある乱数を読み出す。

【００２９】制御回路３は、ステップＳ１７で、EEPROM４のDiscID tableから、ステップＳ３でDiscIDが検出されたのと同一アドレスにある乱数を読み出す。制御回路３は、ステップＳ１８で、ステップＳ１６およびステップＳ１７で検出された乱数が一致するか否かの判定を行う。両者の乱数が一致しないと判定された場合、または、ステップＳ１５で、光ディスク記録再生装置１のDeviceIDが光ディスク１５のDeviceID tableに記録されていないと判定された場合、ステップＳ１９に進み、制御回路３は、光ディスク１５が不正コピーに係るものであると判断する。制御回路３は、この判断に基づき、記録再生回路５を制御して、ユーザデータ信号の記録または再生を禁止させる。すなわち、この場合、制御回路３は、ユーザデータエリアへのアクセスを拒絶する。

【００３０】一方、ステップＳ１８において、ステップＳ１６およびステップＳ１７で読み出された乱数が一致すると判定された場合、図５のステップＳ２０に進み、制御回路３は、以降ステップＳ２８に至るまでの処理を実行するよう各回路を制御する。なお、図５のステップＳ２０乃至Ｓ２８の処理は、図４のステップＳ４乃至Ｓ１２の処理と同様の処理である。この場合、ステップＳ２３およびＳ２７において、DiscIDおよびDeviceIDは、図４のステップＳ３およびＳ１５で読み出されたものと同一のものが書き込まれる。これに対し、ステップＳ２０において、乱数は、図４のステップＳ１７およびＳ１８で読み出されたものとは異なるものが発生され、ステップＳ２４およびＳ２８において書き換えられる。ステップＳ２８の処理の終了後は、図４のステップＳ１３に戻り、制御回路３は、以下同様の処理を実行する。

【００３１】例えば、ステップＳ８で乱数が書き込まれた後、再び、光ディスク記録再生装置１が光ディスク１５にアクセスした場合には、ステップＳ３、およびステップＳ１５でYESと判定されて、ステップＳ１６，Ｓ１７に進み、制御回路３により、乱数が読み出され、ステップＳ１８で、アクセスが許容されることになる。しかしながら、光ディスク１５のIDを不正にコピーした光ディスクが、光記録再生装置１に装着された場合には、仮に、光ディスク記録再生装置のDeviceIDが不正にコピーされていたとしても、ステップＳ１５は（そこでYESと判定されて）通過できるが、ステップＳ１８で、時変情報である乱数が一致しないと判定されてしまうので、ユーザデータへのアクセスが拒絶されることになる。

【００３２】以上のようにして、DiscID tableのDiscIDおよび乱数と、DeviceID tableのDeviceIDおよび乱数を比較し、その一致を検査するようにしたので、ユーザデータエリアへの不正なアクセスに対する防止機能を高めることができる。

【００３３】ところで、コンテンツデータを図６に示すように暗号化することで、不正コピーに対する防御効果をより一層高めることが可能である。

【００３４】すなわち、図６の例では、光ディスク１５のリードインエリアには、DiscIDとDeviceID tableの他、ディスクキーKdをイフェクティブマスタキーKemで暗号化した暗号化ディスクキーEKdが格納されている。

【００３５】なお、イフェクティブマスタキーKemは、式（１）に従い、マスタキーKmとDiscIDの結合にhash関

数を適用して計算される。ここで、ＡとＢの結合とは、例えば、Ａが３２ビットで構成され、Ｂも３２ビットで構成されるとき、Ａの後にＢを配置して、６４ビットのデータとすることを意味する。

イフェクティブマスタキーKem＝hash（マスタキーKm＋DiscID）　　（１）

ここでマスタキーKmは、著作権者等から適正にライセンスを受けた者（光ディスク記録再生装置）にだけ与えられる秘密のキーである。データエリアの各セクタSiは、ヘッダおよびメインデータ部で構成され、ヘッダには、（セクタ毎に異なる）セクタキーKsiをディスクキーKdで暗号化した暗号化セクタキーEKsi(i=1,2,...)が格納されている（ここでKsiのiは、セクタの番号を示し、セクタキーはセクタ毎に異なるのでKsiと記述するが、特に区別する必要がない場合は、Ksとも記述する）。メインデータ部には、コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータが格納されている。

【００３６】次に、図６のようにしてデータが記録されている光ディスク１５を、記録再生する光ディスク記録再生装置１の構成例を、図７に示す。この例では、記録再生回路５が復号部６０と暗号化部６１を有している。その他の構成は図１における場合と同様である。

【００３７】図８は、復号部６０の内部の構成を示す図である。Kem発生モジュール８１のKmメモリ８５は、マスタキーKmを記憶する。Kem発生モジュール８１のhash関数回路８６は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキーKemを計算する。EKd復号回路８２は、光ディスク１５から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを計算する。EKs復号回路８３は、光ディスク１５から各セクタSiのヘッダの暗号化セクタキーEKsiを読み出し、ディスクキーKdで復号して、セクタキーKsiを計算する。コンテンツデータ復号回路８４は、光ディスク１５から読み出された暗号化されたコンテンツデータを、セクタキーKsiで復号する。

【００３８】図９は、暗号化部６１の内部の構成を示す図である。Kem発生モジュール１０１のKmメモリ１０６は、マスタキーKmを記憶する。Kem発生モジュール１０１のhash関数回路８７は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキーKemを計算する。EKd暗号化復号回路１０２は、光ディスク１５から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを得る。乱数発生回路９は、ディスクキーKdおよびセクタキーKsiをそれぞれ乱数として発生する。EKd暗号化復号回路１０２は、ディスクキーKdを、イフェクティブマスタキーKemで暗号化して、光ディスク１５に記録するとともに、光ディスク１５から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号する。Ks暗号化回路１０３は、セクタキーKsiをディスクキーKdで暗号化して暗号化セクタキーEKsiを生成し、光ディスク１５に記録する。コンテンツデータ暗号化回路１０４は、セクタキーKsiで、コンテンツデータを暗号化し、光ディスク１５に記録する。

【００３９】図７の光ディスク記録再生装置１は、基本的に、図４および図５に示した場合と同様の動作を行うので、その説明は省略する。但し、この光ディスク記録再生装置１は、図４のステップＳ１３でのアクセス動作を、図１０または図１１のフローチャートに示すように実行する。

【００４０】図１０は、復号部６０により行われる、ユーザデータの再生処理を説明するフローチャートである。最初に、ステップＳ４１において、Kem発生モジュール８１のhash関数回路８６は、光ディスク１５のリードインエリアから読み出されたDiscIDを受け取る。Kem発生モジュール８１のhash関数回路８６はさらに、ステップＳ４２で、Kmメモリ８５からマスタキーKmを読み出し、上述の式（１）に従い、光ディスク１５のDiscID、および、Kmメモリ８５から読み出したマスタキーKmの結合にhash関数を適用してイフェクティブマスタキーKemを計算し、EKd復号回路８２に供給する。EKd復号回路８２は、ステップＳ４３で、光ディスク１５のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路８２は、ステップＳ４４で、この読み出された暗号化ディスクキーEKdを、hash関数回路８６から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを計算し、EKs復号回路８３に出力する。

【００４１】EKs復号回路８３は、ステップＳ４５で、光ディスク１５のデータエリアから読み出された各セクタの暗号化セクタキーEKsi（i=1,2,...）を受け取る。EKs復号回路８３は、ステップＳ４６で、この読み出された暗号化セクタキーEKsiを、EKd復号回路８２から受け取ったディスクキーKdで復号して、セクタキーKsiを計算し、コンテンツデータ復号回路８４に出力する。コンテンツデータ復号回路８４は、ステップＳ４７で、光ディスク１５から読み出された暗号化されたコンテンツデータを受け取る。コンテンツデータ復号回路８４は、ステップＳ４８で、この読み出されたコンテンツデータを、EKs復号回路８３から受け取ったセクタキーKsiで復号し、出力する。

【００４２】復号部６０の各回路は、ステップＳ４９で、光ディスク１５のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップＳ５０に進み、復号部６０の各回路は、光ディスク１５の、まだ読み出されていない次のセクタのデータの供給を受け、ステップＳ４５以降の処理を繰り返す。全てのコンテンツデータが読み出されたと判定

された場合、復号部６０の各回路は、全ての処理を終了する。

【００４３】図１１は、暗号化部６１により行われる、ユーザデータの記録処理を説明するフローチャートである。最初に、ステップＳ７１において、Kem発生モジュール１０１のhash関数回路１０７は、光ディスク１５のリードインエリアから読み出されたDiscIDを受け取る。Kem発生モジュール１０１のhash関数回路１０７は、ステップＳ７２で、Kem発生モジュール１０１のKmメモリ１０６から、マスタキーKmを読み出す。Kem発生モジュール１０１のhash関数回路８７は、ステップＳ７３で、上述の式（１）に従い、光ディスク１５のDiscID、および、Kmメモリ１０６から読み出したマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、EKd暗号化復号回路１０２に供給する。

【００４４】EKd暗号化復号回路１０２は、ステップＳ７４で、光ディスクのリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd暗号化復号回路１０２は、ステップＳ７５で、光ディスク１５のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か（暗号化ディスクキーEKdを受け取ることができたか否か）の判定を行う。暗号化ディスクキーEKdが書き込まれていないと判定された場合、ステップＳ７６に進み、乱数発生回路９は、４０ビットの乱数を発生し、ディスクキーKdとして、EKd暗号化復号回路１０２に出力する。EKd暗号化復号回路１０２は、ステップＳ７７で、乱数発生回路９から供給されたディスクキーKdを、hash関数回路１０７から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク１５のリードインエリアに記録する。

【００４５】ステップＳ７５で、暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップＳ７８に進み、EKd暗号化復号回路１０２は、この光ディスク１５から読み出された暗号化ディスクキーEKdを、hash関数回路１０７から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。EKd暗号化復号回路１０２は、ディスクキーKdを、Ks暗号化回路１０３に出力する。

【００４６】ステップＳ７７またはＳ７８の処理の後、乱数発生回路９は、ステップＳ７９で、４０ビットの乱数を発生し、セクタキーKsとして、Ks暗号化回路１０３、およびコンテンツデータ暗号化回路１０４に出力する。Ks暗号化回路１０３は、ステップＳ８０で、EKd暗号化復号回路１０２（暗号化ディスクキーEKdが光ディスク１５に記録されている場合）、または乱数発生回路９（暗号化ディスクキーEKdが光ディスク１５に記録されていない場合）から受け取ったディスクキーKdで、乱数発生回路９から受け取ったセクタキーKsiを暗号化して、暗号化セクタキーEKsiを生成する。Ks暗号化回路１０３は、暗号化セクタキーEKsiを、光ディスク１５のデータエリアにあるセクタヘッダに記録する。

【００４７】コンテンツデータ暗号化回路１０４は、ステップＳ８１で、（ステップＳ７９で乱数発生回路９から受け取った）セクタキーKsiにより、コンテンツデータを暗号化し、光ディスク１５のデータエリアのメインデータ部に記録する。

【００４８】暗号化部６１の各回路は、ステップＳ８２で、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータをまだ記録してはいないと判定された場合、ステップＳ８３に進み、暗号化部６１の各回路は、光ディスク１５の、まだデータを記録していないセクタにアクセスし、ステップＳ７９に戻り、以下同様の処理を繰り返す。ステップＳ８２で、全てのコンテンツデータが記録されたと判定された場合、復号部６０の各回路は、全ての処理を終了する。

【００４９】以上のようにして、DiscID tableのDiscIDおよび乱数と、DeviceID tableのDeviceIDおよび乱数を比較し、その一致を検査する第１の実施の形態に加えて、第２の実施の形態では、コンテンツデータを暗号化させることでユーザデータエリアへの不正なアクセスをさらに困難にしたので、不正コピーに対する防御効果をさらに高めることができる。

【００５０】本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【００５１】なお、本明細書中において、上記処理を実行するコンピュータプログムをユーザに提供する提供媒体には、磁気ディスク、CD-ROMなどの情報記録媒体の他、インターネット、デジタル衛星などのネットワークによる伝送媒体も含まれる。

【００５２】

【発明の効果】以上のように、請求項１に記載の情報処理装置、請求項２に記載の情報処理方法、および請求項３に記載の提供媒体によれば、記録媒体に対してアクセスした情報処理装置の第１のテーブルの内容と、記録媒体から読み出された第２のテーブルの内容を比較し、その比較結果に対応して記録媒体に対するアクセスを制御するようにしたので、より安全にデータを授受し、著作権者の権利を保護することができる。

【００５３】また、請求項４に記載の記録媒体によれば、記録媒体に固有のID、装着された情報処理装置のID、および情報処理装置が発生した時変情報とが記録されるようにしたので、より安全にデータを授受し、著作権者の権利を保護することができる。

【図面の簡単な説明】

【図１】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

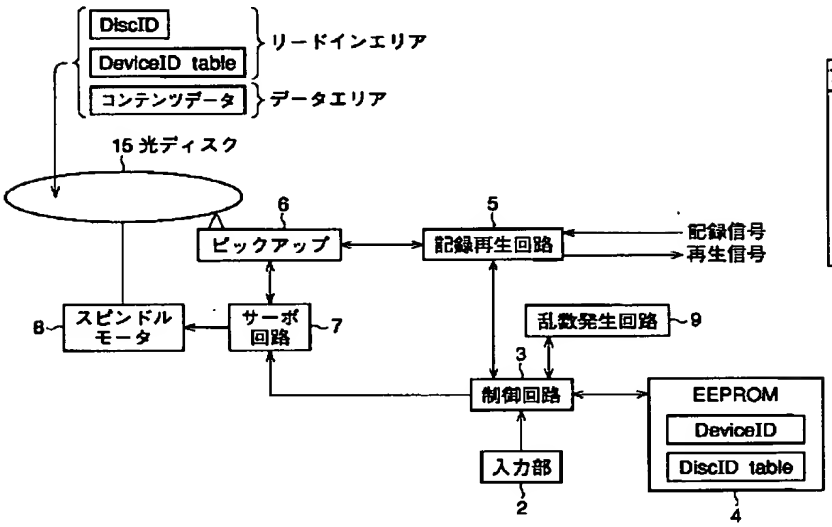
【図２】DeviceID tableの例を示す図である。

【図３】DiscID tableの例を示す図である。

【図４】図１の光ディスク記録再生装置１の動作を説明

するフローチャートである。
【図５】図１の光ディスク記録再生装置１の動作を説明するフローチャートである。
【図６】光ディスクに記録するデータを説明する図である。
【図７】本発明を適用した光ディスク記録再生装置の他の実施の形態の構成を示すブロック図である。
【図８】図７の復号部６０の内部の構成を示す図である。
【図９】図７の暗号化部６１の内部の構成を示す図である。
【図１０】図８の復号部６０の動作を説明するフローチャートである。
【図１１】図９の暗号化部６１の動作を説明するフローチャートである。
【符号の説明】
１　光ディスク記録再生装置，　２　入力部，　３　制御回路，　４　EEPROM，　５　記録再生回路，　６　ピックアップ，　７　サーボ回路，　８　スピンドルモータ，　９　乱数発生回路，　１５　光ディスク，　６０　復号部，　６１　暗号化部，，　８１　Kem発生モジュール，　８２　EKd復号回路，　８３　EKs復号回路，　８４　コンテンツデータ復号回路，　８５　Kmメモリ，　８６hash関数回路，　１０１　Kem発生モジュール，　１０２　EKd暗号化復号回路，１０３　Ks暗号化回路，　１０４　コンテンツデータ暗号化回路，　１０６　Kmメモリ，　１０７　hash関数回路

【図１】



【図２】

DeviceID table

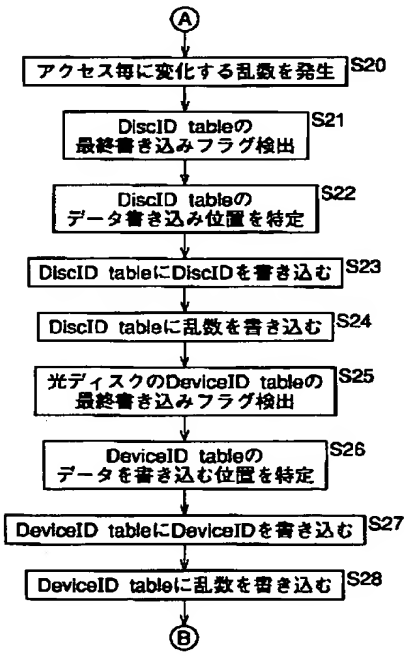
アドレス	DeviceID	乱数	最終書き込みフラグ
1			
2			
・			
・			
・			
・			
100			

【図３】

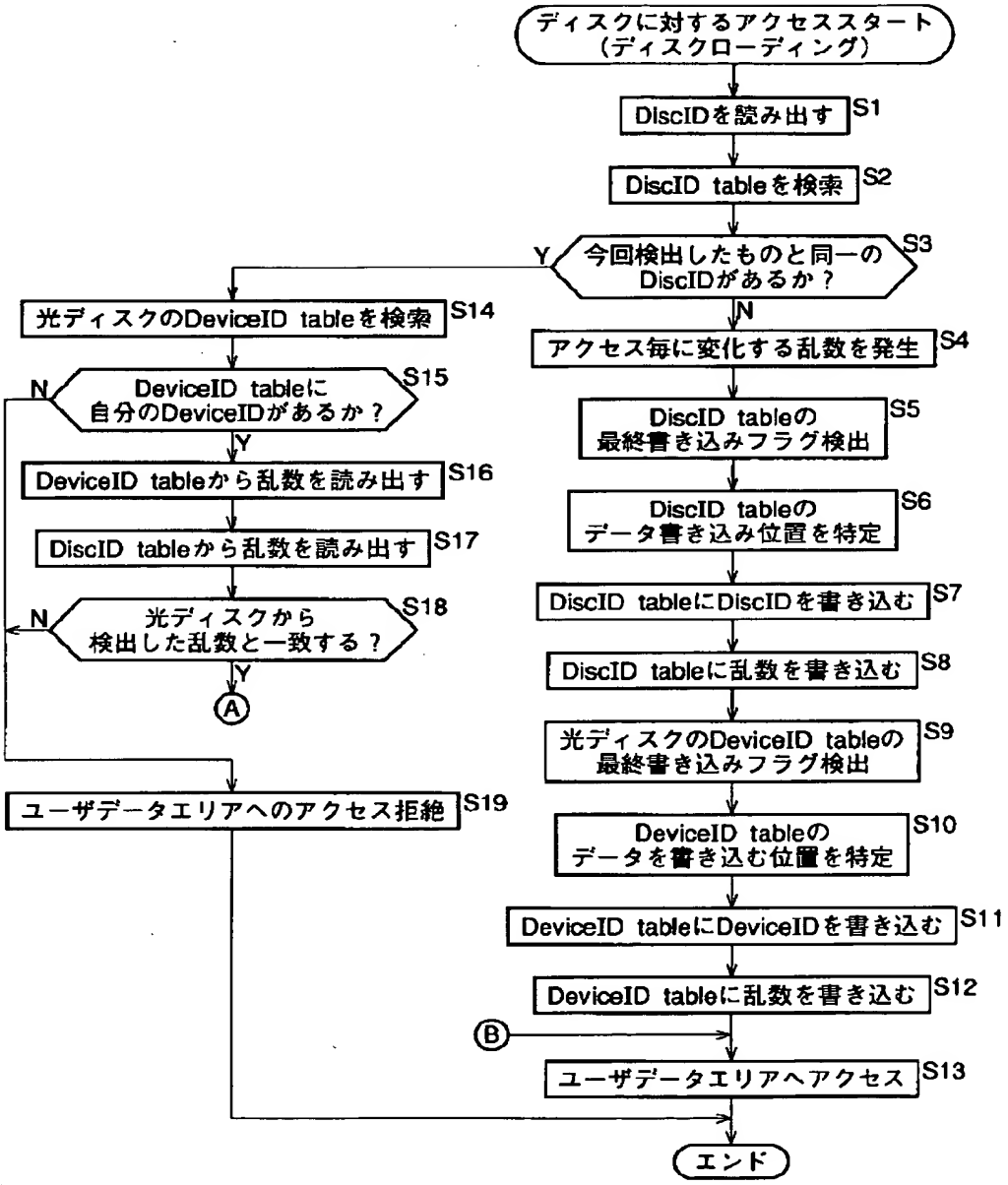
DiscID table

アドレス	DiscID	乱数	最終書き込みフラグ
1			
2			
・			
・			
・			
・			
100			

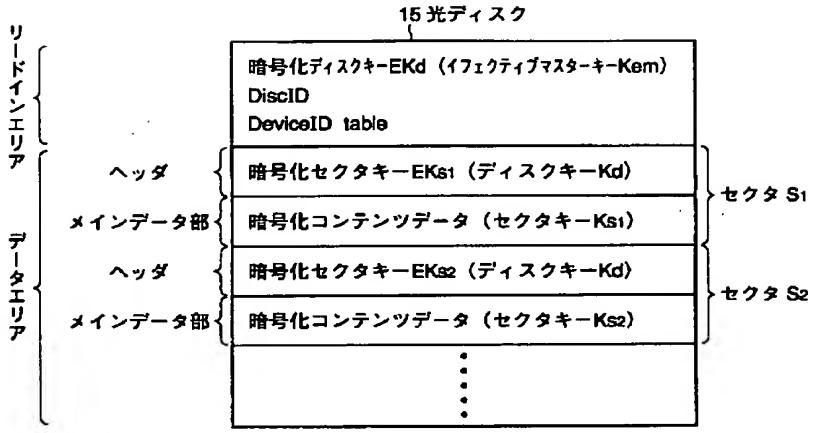
【図５】



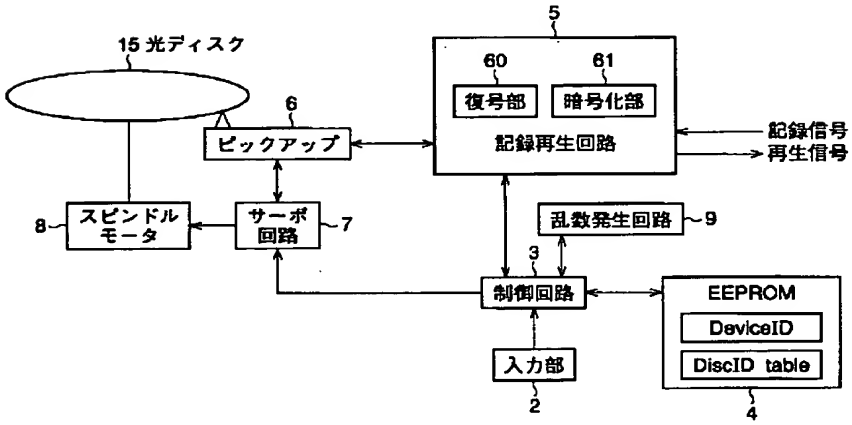
【図４】


ディスクに対するアクセススタート
（ディスクローディング）
DiscIDを読み出す
S1
DiscID tableを検索
S2
今回検出したものと同一の
DiscIDがあるか？
S3
Y
N
光ディスクのDeviceID tableを検索
S14
アクセス毎に変化する乱数を発生
S4
N
DeviceID tableに
自分のDeviceIDがあるか？
S15
DiscID tableの
最終書き込みフラグ検出
S5
Y
DeviceID tableから乱数を読み出す
S16
DiscID tableの
データ書き込み位置を特定
S6
DiscID tableから乱数を読み出す
S17
DiscID tableにDiscIDを書き込む
S7
N
光ディスクから
検出した乱数と一致する？
S18
DiscID tableに乱数を書き込む
S8
Y
Ⓐ
光ディスクのDeviceID tableの
最終書き込みフラグ検出
S9
ユーザデータエリアへのアクセス拒絶
S19
DeviceID tableの
データを書き込む位置を特定
S10
DeviceID tableにDeviceIDを書き込む
S11
DeviceID tableに乱数を書き込む
S12
Ⓑ
ユーザデータエリアへアクセス
S13
エンド

【図６】

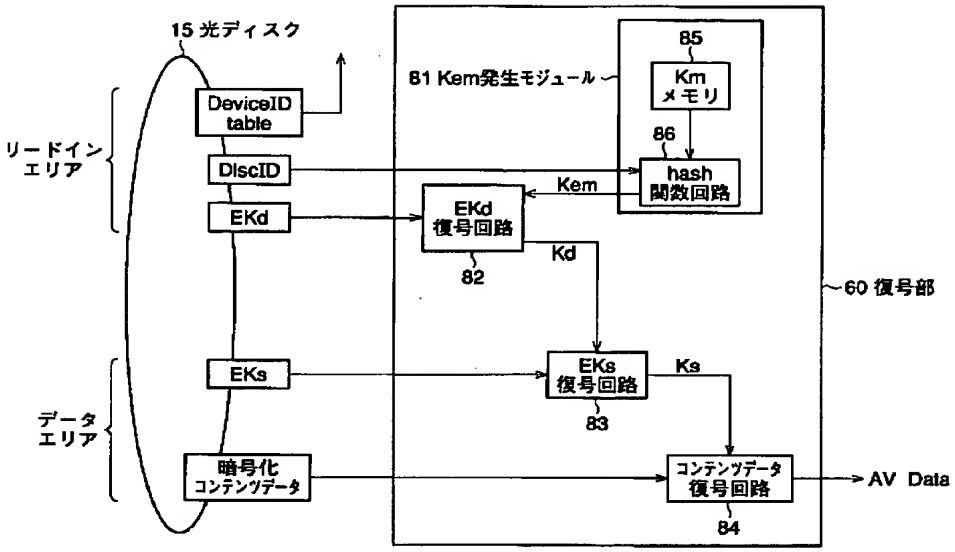


【図７】

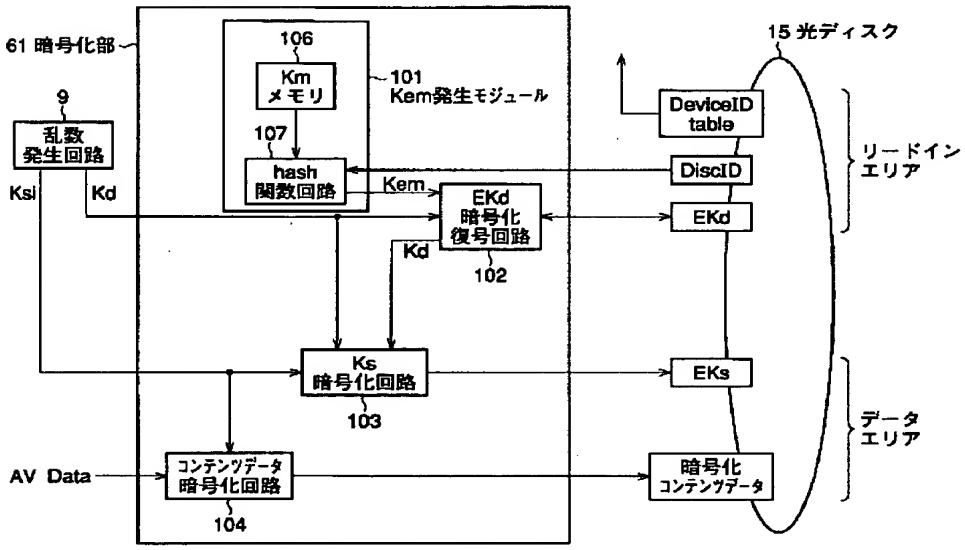


光ディスク記録再生装置 1

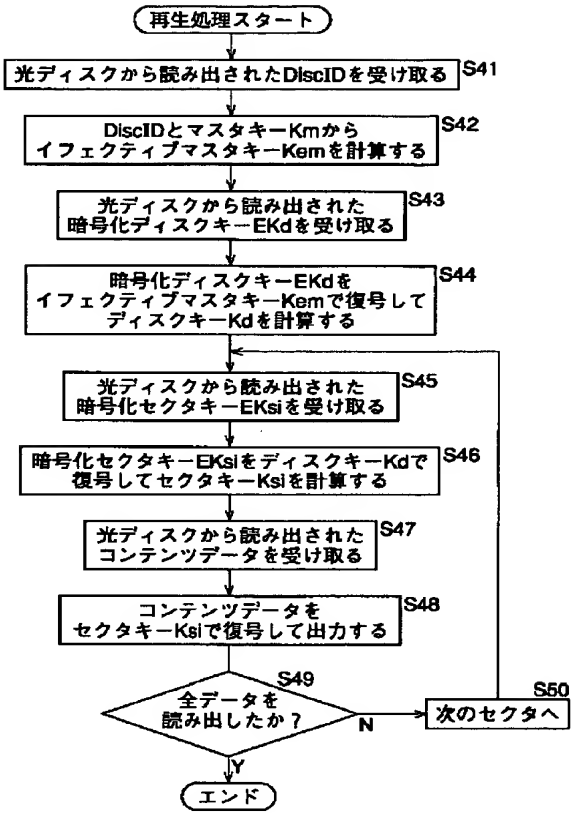
【図８】


15 光ディスク
リードイン エリア
データ エリア
DeviceID table
DiscID
EKd
EKs
暗号化 コンテンツデータ
81 Kem発生モジュール
85
Km メモリ
86
hash 関数回路
Kem
EKd 復号回路
82
Kd
EKs 復号回路
83
Ks
コンテンツデータ 復号回路
84
AV Data
60 復号部

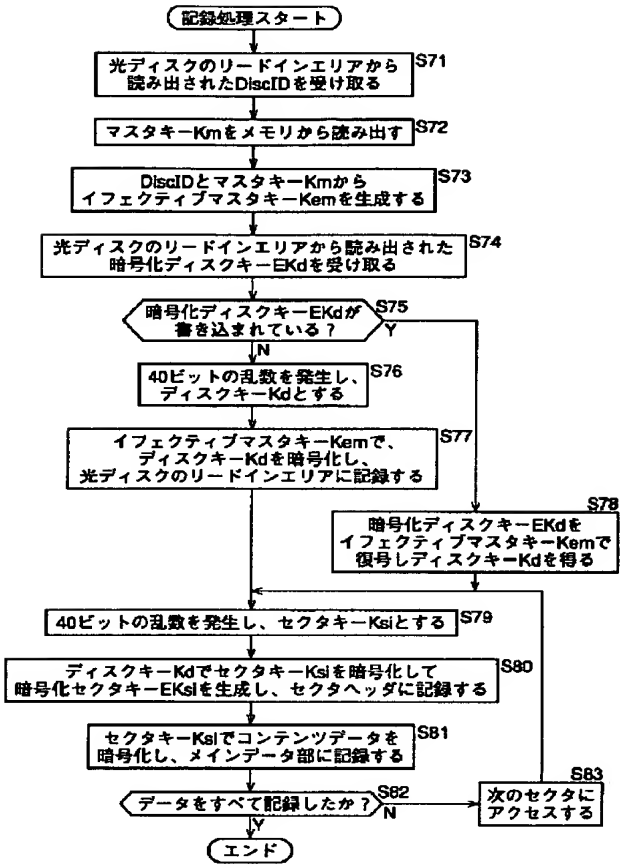
【図９】


61 暗号化部
9
乱数 発生回路
Ksi
Kd
106
Km メモリ
107
hash 関数回路
101 Kem発生モジュール
Kem
EKd 暗号化 復号回路
102
Kd
Ks 暗号化回路
103
AV Data
コンテンツデータ 暗号化回路
104
15 光ディスク
DeviceID table
DiscID
EKd
EKs
暗号化 コンテンツデータ
リードイン エリア
データ エリア

【図１０】



【図１１】



フロントページの続き

(51)Int.Cl.[6]	識別記号	ＦＩ
Ｇ１１Ｂ　20/12		Ｇ１１Ｂ　20/12